



Best Practices Guide

# McAfee Endpoint Encryption for PC 6.2 Software

For use with ePolicy Orchestrator 4.5, 4.6 Software

## **COPYRIGHT**

Copyright © 2012 McAfee, Inc. Do not copy without permission.

## **TRADEMARK ATTRIBUTIONS**

McAfee, the McAfee logo, McAfee Active Protection, McAfee AppPrism, McAfee Artemis, McAfee CleanBoot, McAfee DeepSAFE, ePolicy Orchestrator, McAfee ePO, McAfee EMM, McAfee Enterprise Mobility Management, Foundscore, Foundstone, McAfee NetPrism, McAfee Policy Enforcer, Policy Lab, McAfee QuickClean, Safe Eyes, McAfee SECURE, SecureOS, McAfee Shredder, SiteAdvisor, SmartFilter, McAfee Stinger, McAfee Total Protection, TrustedSource, VirusScan, WaveSecure, WormTraq are trademarks or registered trademarks of McAfee, Inc. or its subsidiaries in the United States and other countries. Other names and brands may be claimed as the property of others.

## **LICENSE INFORMATION**

### **License Agreement**

NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANY YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEBSITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO MCAFFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.

# Contents

	<b>Preface</b>	<b>5</b>
	About this guide . . . . .	5
	Audience . . . . .	5
	Conventions . . . . .	5
	Find product documentation . . . . .	6
<b>1</b>	<b>Introduction</b>	<b>7</b>
	Purpose of this guide . . . . .	7
	Abbreviations . . . . .	7
<b>2</b>	<b>Design philosophy</b>	<b>9</b>
	Support for the self-encrypting (Opal from Trusted Computing Group) drive . . . . .	9
	EEPC Policies . . . . .	10
	Configure UBP enforcement . . . . .	10
	PBA in EEPC 6.2 . . . . .	11
	How Endpoint Encryption works . . . . .	11
	McAfee ePO requirements . . . . .	11
<b>3</b>	<b>Software configuration and policies</b>	<b>13</b>
	Active Directory configuration . . . . .	14
	EE LDAP Server User/Group Synchronization . . . . .	16
	Recommended Product Settings Policy . . . . .	18
	Recommended User-Based Policy Settings . . . . .	22
	Phased deployment strategies . . . . .	24
<b>4</b>	<b>Deployment and activation</b>	<b>27</b>
	Basic preparations and recommendations . . . . .	28
	High level process of the installation . . . . .	29
	Client task to deploy the EEAgent and EEPC packages . . . . .	30
	Add group users . . . . .	31
	Users . . . . .	31
	Add local domain users . . . . .	31
	EEPC activation sequence . . . . .	33
	Activate EEPC using Add local domain users . . . . .	34
<b>5</b>	<b>Operations and maintenance</b>	<b>35</b>
	How does disabling/deleting a user in Active Directory affect the EEPC user . . . . .	35
	Manage Machine Keys . . . . .	36
	Configure role based access control for managing EEPC . . . . .	38
	EEPC 6.2 scalability . . . . .	39
<b>6</b>	<b>Migration and upgrade</b>	<b>41</b>
	Best practices for migration and upgrade . . . . .	41
	Export user assignments from 5.x.x database . . . . .	43
	Import user assignments to McAfee ePO . . . . .	44

Upgrade to EEPC 6.2 . . . . .	45
<b>7 Use ePolicy Orchestrator to report client status</b>	<b>47</b>
Track the progress of the deployment and encryption status . . . . .	47
Report encryption status from McAfee ePO . . . . .	47
<b>Index</b>	<b>49</b>

# Preface

This guide provides the information on best practices on using EEPC.

## Contents

- ▶ *About this guide*
- ▶ *Find product documentation*

---

## About this guide

This information describes the guide's target audience, the typographical conventions and icons used in this guide, and how the guide is organized.

## Audience

McAfee documentation is carefully researched and written for the target audience.

The information in this guide is intended primarily for:

- **Administrators** — People who implement and enforce the company's security program.
- **Users** — People who use the computer where the software is running and can access some or all of its features.

## Conventions

This guide uses the following typographical conventions and icons.

*Book title or Emphasis* Title of a book, chapter, or topic; introduction of a new term; emphasis.

**Bold** Text that is strongly emphasized.

User input or Path Commands and other text that the user types; the path of a folder or program.

`Code` A code sample.

**User interface** Words in the user interface including options, menus, buttons, and dialog boxes.

Hypertext blue A live link to a topic or to a website.



**Note:** Additional information, like an alternate method of accessing an option.



**Tip:** Suggestions and recommendations.



**Important/ Caution:** Valuable advice to protect your computer system, software installation, network, business, or data.



**Warning:** Critical advice to prevent bodily harm when using a hardware product.

---

## Find product documentation

McAfee provides the information you need during each phase of product implementation, from installation to daily use and troubleshooting. After a product is released, information about the product is entered into the McAfee online KnowledgeBase.

### Task

- 1 Go to the McAfee Technical Support ServicePortal at <http://mysupport.mcafee.com>.
- 2 Under **Self Service**, access the type of information you need:

To access...	Do this...
User documentation	<ol style="list-style-type: none"><li>1 Click <b>Product Documentation</b>.</li><li>2 Select a product, then select a version.</li><li>3 Select a product document.</li></ol>
KnowledgeBase	<ul style="list-style-type: none"><li>• Click <b>Search the KnowledgeBase</b> for answers to your product questions.</li><li>• Click <b>Browse the KnowledgeBase</b> for articles listed by product and version.</li></ul>

# 1

## Introduction

McAfee Endpoint Encryption for PC (EEPC) provides superior encryption across a variety of endpoints such as desktops and laptops. The EEPC solution uses strong access control with Pre-Boot Authentication (PBA) and a NIST approved algorithm to encrypt data on endpoints. Encryption and decryption are completely transparent to the end user and performed without hindering system performance.

Administrators can easily implement and enforce security policies that control how sensitive data is encrypted. These policies allow the administrators to monitor real-time events and generate reports to demonstrate compliance with internal and regulatory requirements.

EEPC has the advantage over other competitive encryption products, because it engages encryption prior to loading of the Windows operating system, while data is at rest.

---

### Purpose of this guide

This guide suggests best practices for deployment and activation. It also discusses optimization and maintenance before and after deployment.

When planning a large scale deployment of EEPC 6.2, it is important to understand:

- The features of McAfee® ePolicy Orchestrator® (McAfee ePO™)
- The process of scaling the back end component
- AD/LDAP
- The associated Endpoint Encryption communication

This document encapsulates the professional opinions of Endpoint Encryption certified engineers, and is not an exact science. You must understand both the product and the environment in which it will be used, before deciding on an implementation strategy. Calculations and figures in this guide are based on field evidence and not theoretical system testing; they are our **best advice** at the time of writing.



Please review the best practices and use the guidelines that best fit your environment.

### Abbreviations

The following table lists the abbreviations used in this document.

**Table 1-1 Abbreviations**

<b>Titles</b>	<b>Designations</b>
AD	Active Directory
ASCI	Agent Server Communication Interval
BIOS	Basic Input/Output System
DN	Domain Name

**Table 1-1 Abbreviations** *(continued)*

<b>Titles</b>	<b>Designations</b>
EEM	Endpoint Encryption Manager
EEPC	Endpoint Encryption for PC
ePO	ePolicy Orchestrator
LDAP	Lightweight Directory Access Protocol
MBR	Master Boot Record
NIST	National Institute of Standards and Technology
OS	Operating System
OU	Organizational Unit
PC	Personal Computer
SSO	Single Sign On
UBP	User-Based Policy



# 2

## Design philosophy

The McAfee ePO server is a central store of configuration information for all systems, servers, policies, and users.

Each time the administrator initiates a policy update, or an Agent Server Communication Interval (ASCI), the EEPC protected system connects with McAfee ePO.

The Endpoint Encryption protected system queries McAfee ePO for any configuration updates and downloads them. An example of updates are a new user assigned (by the administrator) to the client system, a change in policies, or a change in server settings specified by the administrator.

The Endpoint Encryption protected system also updates any changes on the client system back to the McAfee ePO server, for example, change of user's password token data.

### Contents

- ▶ *Support for the self-encrypting (Opal from Trusted Computing Group) drive*
- ▶ *EEPC Policies*
- ▶ *PBA in EEPC 6.2*
- ▶ *How Endpoint Encryption works*
- ▶ *McAfee ePO requirements*

---

## Support for the self-encrypting (Opal from Trusted Computing Group) drive

EEPC 6.2 provides better management facility for the Opal drive, which is a self-contained and standalone Hard Disk Drive (HDD) that conforms to the Trusted Computing Group (TCG) Opal standard.

The Opal drive is always encrypted by the on board crypto processor. However, it may or may not be locked. Though the Opal drive handles all of the encryption, it needs to be managed by a management software like McAfee ePolicy Orchestrator. If the Opal drive is not managed, it behaves and responds like a normal HDD.

The combination of EEPC and McAfee ePO for Opal provides:

- Centralized management
- Reporting and recovery functionality
- A secure Pre-Boot Authentication that unlocks the Opal drive
- An efficient user management
- Continuous policy enforcement

The overall experience and tasks of an administrator and users in installing and using EEPC are exactly the same regardless of whether the target system has an Opal drive or a normal HDD. The installation of the product extension, deployment of the software packages, policy enforcement, and the method of management are all the same for both systems with Opal and HDD.

---

## EEPC Policies

EEPC is managed through the McAfee ePO server, using a combination of Product Settings and User-Based Policies.

The McAfee ePO console allows the administrator to enforce policies across groups of computers, or a single computer. Any new policy enforcement through McAfee ePO overrides the existing policy that is already set on the individual systems. There are two types of policies: Product Settings and User-Based Policies. Product Settings Policies are specific to a system or a group of systems. User-Based Policies are specific to a user, or a group of users, on a system or a group of systems.

The Product Settings Policy controls the behavior of the EEPC installed systems. For example, it contains the options for enabling encryption, enabling automatic booting, and controlling the theme for the Pre-Boot environment.

The User-Based Policy controls the parameters for EEPC user accounts. For example, it contains the options for selecting a token type (including password and smartcard) and password content rules.

### Configure UBP enforcement

By default, all users inherit the default User-Based Policy assigned to a system and are prevented from using Policy Assignment Rules for EEPC UBP in order to provide maximum system scalability. User-Based policies should be kept to a minimum when possible since UBPs impact performance and activation time.

#### Before you begin

You must have appropriate permissions to perform this task.

To allow a user to use a non-default User Based Policy, you must enable UBP enforcement for that user. This allows Policy Assignment Rules to be executed to select a specific non-default UBP for the user. If not enabled, Policy Assignment Rules are not performed and the user inherits the default UBP.

**CAUTION:** Failing to assign UBP using Policy Assignment Rule to users, with UBP enforcement enabled, might cause EEPC activation to fail.

#### User Based Policies in EEPC 6.2

A requirement of EEPC 6.2 is that you need to specify which groups of users are allowed or not to use the Policy Assignment Rules. The allowed users get their required User Based Policies. Users that are not allowed to use the Policy Assignment Rules inherit the default User Based Policies assigned to the system.

#### Task

- 1 Click **Menu | Reporting | Queries**. The Queries page opens.
- 2 Select **Endpoint Encryption** from Shared Groups in Groups pane. The standard EE query list appears.
- 3 Run the **EE: Users** query to list all the Endpoint Encryption Users.
- 4 Select a user(s) from the list to enforce the policy.

- 5 Click **Actions** | **Endpoint Encryption** | **Configure UBP enforcement**. The Configure UBP enforcement page appears with Enable and Disable options.
- 6 Select **Enable** or **Disable**, then click **OK** to configure the UBP enforcement state. On selecting Enable, Policy Assignment Rules are enabled for the selected users, and a specific UBP is assigned to the user according to the rule defined.



At each ASCI, ePolicy Orchestrator enforces all the relevant user-based policies to each client in addition to the user-based policy for the logged on user configured with UBP enforcement.

---

## PBA in EEPC 6.2

PBA in EEPC is part of a mini operating system that acts as a trusted authentication layer by serving as an extension of the BIOS, or boot firmware, and guarantees a secure, tamper-proof environment external to the Microsoft Windows operating system.

The PBA prevents Windows from loading until the user has authenticated with the correct password. It eliminates the possibility that one of the millions of lines of the OS code can compromise the privacy of personal or company data.

The PBA provided by EEPC has proven time and time again as the best Data Protection solution in the market. The PBA solution is an unmatched best practice to be followed by any organization for system security and data protection.

---

## How Endpoint Encryption works

A boot sequence is executed by the BIOS leading to the starting of the bootable operating systems.

The boot sequence is the initial set of operations that the computer performs when it is switched on. A boot loader (or a bootstrap loader) is a short computer program that loads the main operating system for the computer. The BIOS first looks at a boot record, which is the logical area **zero** (or starting point) point of the disk drive, known as Master Boot Record (MBR), which contains the boot loader.

EEPC alters the MBR; the BIOS loads the modified MBR that will then load the sector chain containing the Pre-Boot environment. This Pre-Boot screen then prompts the user for authentication credentials, which might be a password, smart card, or token.

After the user enters valid authentication credentials, the operating system starts to load and the user can use the computer in a normal way.

Encrypting a PC with EEPC 6.2 is the best and the most important practice that any organization can have for protecting their data.

---

## McAfee ePO requirements

The McAfee ePO server is a central store of configuration information for all systems, servers, policies, and users. It can be installed only on Windows Server 2003 or 2008 operating systems. For detailed

information about installing or using McAfee ePO, see the ePolicy Orchestrator product documentation for versions 4.5 and 4.6.

### **Supported environments for McAfee ePO and EEPC**

As new operating systems and service packs are released, the original Product Guides for McAfee ePO and EEPC might not reflect the current McAfee support policy for those platforms. To view supported environments for McAfee ePO and EEPC, read the Knowledge Base article <https://kc.mcafee.com/corporate/index?page=content&id=KB51109>, or refer to the *McAfee Endpoint Encryption - 6.2 (EEPC) and 1.1 (EEMac) Product Guide*.

### **Hardware requirements for McAfee ePO**

For details on the hardware requirements for McAfee ePO, see the ePolicy Orchestrator product documentation for versions 4.5 and 4.6.

### **Software requirements**

For details on the software requirements for McAfee ePO and McAfee Agent, see the *McAfee Endpoint Encryption - 6.2 (EEPC) and 1.1 (EEMac) Product Guide*.



Clients communicating with McAfee ePO 4.0, 4.5, and 4.6 through VPN disappear from the McAfee tree. For more information, refer to the KnowledgeBase article <https://kc.mcafee.com/corporate/index?page=content&id=KB52949>.

# 3

## Software configuration and policies

When planning for a rollout and deployment of EEPC, we recommend that you understand the following important tasks correctly.

- How to configure an LDAP server in McAfee ePO
- How to schedule and run the **EE LDAP Server User/Group Synchronization** task
- How to configure policies and different strategies for phased deployments

### Contents

- ▶ *Active Directory configuration*
- ▶ *EE LDAP Server User/Group Synchronization*
- ▶ *Recommended Product Settings Policy*
- ▶ *Recommended User-Based Policy Settings*
- ▶ *Phased deployment strategies*

## Active Directory configuration

EEPC users are not created from the McAfee ePO server. They are assigned to the client systems from an Active Directory (AD) registered in ePolicy Orchestrator. The McAfee ePO Server is responsible for the connection between the client and AD.



Check for the correct format of the Domain name, Username, and Server Address while registering the LDAP server in McAfee ePO.

The AD users are different from EEPC users.

- A user exists in AD.
- User string is added as a Pre-Boot user.
- User string is then matched to AD to verify if it exists.



- User string is used to login into Pre-Boot.
- If the correct SSO options are selected, then the user string is compared [string comparison **similar** to java **string.matches()**].
- The end user perceives that he is logging only once using a single user, however, the underlying mechanism still uses two different users one to logon at Pre-Boot and another to logon against Active Directory.

Registered Server Builder	1. Description
LDAP server type:	Active Directory
Server name:	<input type="radio"/> Domain name: <input type="text" value="dlp.com"/> Use DNS-style domain name. <input checked="" type="radio"/> Server name: <input type="text" value="172.19.193.45"/> Use servername or IP address.
Port number:	<input type="text"/>
Use SSL:	<input type="checkbox"/>
User name:	<input type="text" value="dlp\neha"/> Use domain\username for Active Directory accounts.
Password:	<input type="checkbox"/> Change password: Password: <input type="text"/> Confirm password: <input type="text"/>
<input type="button" value="Test Connection"/> Successfully connected to the LDAP server.	

**Figure 3-1 Register Active Directory**



It is better to key in the IP address of the domain server in the Server name field than entering the domain name of the domain server. This is due to the potential problems caused by DNS failures and/or canonical DNS servers failing to resolve the LDAP server(s) for the domain.

There could be instances when the Test Connection would get through even if you haven't keyed in the domain name and the username in correct format, however, the error could hinder the EEPC activation. One of the potential outcomes is that a successful logon to the LDAP server might work because the DNS resolves to LDAP\_A but when the task is run the DNS resolves to LDAP\_B and the logon fails. Other potential outcomes can be that the logon happens against a LDAP server containing the full copy of the AD structure, a later resolution points to a newly added server that only contains a subset of the AD structure.

The McAfee ePO server allows the administrator to filter user accounts that can be imported into EEPC, based on a portion of LDAP. For example, if the configured LDAP has two major Organizational Units (OUs): OU=My OU and OU=Phils\_OU and if only the user accounts from OU=My OU need to be imported then it can be achieved easily using ePO Server.

Select specific OUs or Group(s) while assigning users using **Menu | Data Protection | Encryption Users | Actions | Endpoint Encryption | Add User(s)** option. The Add User(s) page provides three options such as **Users**, **From the groups**, and **From the organizational units** with recursive option for Groups and OUs. You can click on the corresponding **Browse** button and list the Users/Groups/OUs present in the configured LDAP server.



The **Recursive** option, if selected, adds the users of the sub groups and Sub OUs in the selected groups and OUs.

**Figure 3-2 Add EE users**

Name	Attribute	Distinguished Name
<input type="checkbox"/> Domain Controllers	Domain Controllers	OU=Domain Controllers,DC=epotest,DC=net
<input type="checkbox"/> McAfee	McAfee	OU=McAfee,DC=epotest,DC=net
<input checked="" type="checkbox"/> My OU	My OU	OU=My OU,DC=epotest,DC=net
<input checked="" type="checkbox"/> Phils_OU	Phils_OU	OU=Phils_OU,DC=epotest,DC=net

**Figure 3-3 Assigning users from OUs**

## EE LDAP Server User/Group Synchronization

Make sure you use the correct user attribute format in the EE LDAP Server User/Group Synchronization task. Match the correct user attributes in the fields.

1. Actions: EE LDAP Server User/Group Synchronization	
LDAP Server	epotest
User Name	samaccountname
Display Name	name
Account Control	useraccountcontrol
User Certificate	usercertificate

**Figure 3-4 EE LDAP Server User/Group Synchronization**

### Username

The value of this field determines the form of the PBA username. For example, if the username value is set to `samaccountname`, the user has to provide the `samaccountname` at the PBA and EE Windows Logon pages.

### Display Name

The value of this field decides the form of the username displayed in ePolicy Orchestrator (**Menu | Reporting | Queries | Endpoint Encryption | EE: Users** and **Menu | Data Protection | Encryption Users | Actions | Endpoint Encryption | View Users**) pages. For example, if the username attribute is set to `samaccountname` and Display Name attribute is set to `userprincipalname`, the username appears as `(paul)@domain.com`.

If the Display name attribute is set to `userprincipalname`, the username appears as `name (paul)@mcafee.com` whereas the user will be allowed to log on with the name value `name (paul)`. (This can be different depending on the attribute selected in the username field and value of the attribute set in the LDAP).

### Account Control

This attribute checks for the status of the user, for example, if the user is enabled or disabled on the LDAP server.



Make sure to select the `useraccountcontrol` attribute in the Account Control field. Attributes other than this do not activate EEPC on the client.



## User Certificate

The User Certificate attribute is used by the McAfee ePO Server to determine which certificate should be sent from ePolicy Orchestrator to the client, for example, smartcard tokens. It is better to clear this attribute when you use the Password only token. Setting this attribute can accumulate large amount of certificate data in the ePO database and impact LDAP performance; therefore, you can remove the certificate query from EE LDAP Server User/Group Synchronization while using the Password only token.



If the attribute value used for username or Display Name is not set in the LDAP server for any user, EEPC uses the attribute distinguished name for that particular object.

After changing the attribute value for any of the fields, the EE LDAP Server User/Group Synchronization task needs to be run, to make sure the ePolicy Orchestrator database is updated with the new values.

## EE LDAP Server User/Group Synchronization task log

The administrator can also view a log of this particular server task by double clicking the particular server task on the Server Task Log page in ePolicy Orchestrator. This log displays only high level information about the users, groups or OUs, and not the detailed log; however, when an LDAP user assigned to **EE: Users** is deleted/disabled from the LDAP server, then the **EE LDAP Server User/Group Synchronization** task log shows the user information of the removed user account.

Server Task Log Details		
Server Task Log Information		
Name:	EE LDAP Sync	
Source:	Server Task	
Start Date:	7/21/10 3:10:30 PM	
Duration:	Less than a minute	
User Name:	admin	
Status:	Completed	
Log Messages	Subtasks	
7/21/10 3:10:31 PM		Started: Synchronizing LDAP information for [epotest].
7/21/10 3:10:31 PM		Started: Checking for unreferenced groups
7/21/10 3:10:31 PM		Completed: Checking for unreferenced groups
7/21/10 3:10:31 PM		Started: Adding recursive groups
7/21/10 3:10:31 PM		Completed: Adding recursive groups
7/21/10 3:10:31 PM		Started: Synchronizing groups
7/21/10 3:10:31 PM		Completed: Synchronizing groups
7/21/10 3:10:31 PM		Started: Checking for unreferenced users
7/21/10 3:10:31 PM		Completed: Checking for unreferenced users
7/21/10 3:10:31 PM		Started: Synchronizing users
7/21/10 3:10:32 PM		Completed: Synchronizing users
7/21/10 3:10:32 PM		Completed: Synchronizing LDAP information for [epotest].

Figure 3-5 Server Task Log





---

## Recommended Product Settings Policy




The Product Settings Policy controls the behavior of the EEPC client. For example, it contains the options for enabling encryption, enabling automatic booting, and controlling the theme for the Pre-Boot environment.

You can configure the Product Settings Policies by navigating through **Menu | Policy | Policy Catalog**, then selecting **Endpoint Encryption 1.2.0** from the Product drop-down list. Select **Product Settings** from the Category drop-down list. Locate the My Default policy and click **Edit Settings**. For more information about individual policy setting, see the *McAfee Endpoint Encryption - 6.2 (EEPC) and 1.1 (EEMac) Product Guide*.


**Table 3-1 Recommended Product Settings Policies**

Policy Options	Recommendations
General Tab	<ul style="list-style-type: none"> <li>• <b>Enable Policy</b> — Leave this option checked (enabled). This policy should be enabled to activate EEPC on the client system. This option needs to be disabled to uninstall EEPC from the client.</li> <li>• <b>Logging Level</b> — Set the required logging level. <ul style="list-style-type: none"> <li> To overwrite the logging level defined in ePolicy Orchestrator, the <b>LoggingLevelOverride</b> registrykey needs to be set.</li> <li>• <b>None</b> — Setting this option does not create any log.</li> <li>• <b>Error</b> — Setting this option logs the error messages only.</li> <li>• <b>Error and Warnings</b> — Setting this option logs the error and warning messages.</li> <li>• <b>Error, Warnings, and Informational</b> — Setting this option logs the error and warning messages with more descriptions.</li> <li>• <b>Error, Warnings, Informational and Debug</b> — Setting this option logs the error and warning messages with more descriptions in the debug mode. We recommend that you enable this option for a detailed logging.</li> </ul> </li> <li>• <b>Allow Temporary Automatic Booting</b> — Leave this option unchecked (disabled). This option allows the administrator to run the scripts on the client system, so that it can automatically boot without prompting for a PBA temporarily. <ul style="list-style-type: none"> <li> If you enable this option, be aware that the McAfee Endpoint Encryption software doesn't protect the data on the drive when it is not in use.</li> </ul> </li> <li>• <b>Expire Uninitialized Users</b> — Leave this option checked (enabled). Allows the administrator to control and manage the user accounts, which are not enrolled or initialized on the client system. Enabling this option forces the user account, that is not initialized, to expire after a number of days as set in the policy.</li> <li>• <b>Allow Machine Information Collection</b> — Leave this option checked (enabled). Enabling this option allows the user to collect the client system details such as the list of assigned users, policy settings, recovery, and Endpoint Encryption Status.</li> </ul>
Encryption Tab	<ul style="list-style-type: none"> <li>• <b>Encrypt — All Disks</b> is a recommended option (The <b>None</b> option does not initiate the encryption). The Encryption type options like <b>None</b>, <b>All Disks except Boot Disk</b>, and <b>Selected Partitions</b> are not applicable to the self-encrypting (Opal) drives.</li> <li>• <b>Selected Partitions</b> — Allows you to select the required partition of the client system and assign it to be encrypted. You can select the required partition by specifying the Windows drive letter or volume name. <ul style="list-style-type: none"> <li> The Partition level encryption is not applicable to the client system that has Opal drives only.</li> </ul> </li> <li>• <b>Encryption Provider Priority</b> — This table also lists the encryption providers (PC Software and Opal) available with the software. You can change and set the encryption priority by moving the encryption provider rows up and down, as appropriate. <ul style="list-style-type: none"> <li> Make sure that you select the required encryption type, as appropriate. Policy enforcement might fail on client systems if you select an unsupported encryption type.</li> </ul> </li> </ul>

**Table 3-1 Recommended Product Settings Policies** *(continued)*

Policy Options	Recommendations
Log On Tab	<ul style="list-style-type: none"> <li data-bbox="443 306 1526 520">• <b>Enable Automatic Booting</b> — Leave this option unchecked (disabled). If you enable this feature, the client system does not have the PBA. This is normally referred as Autoboot mode. It could be useful to enable this option when the administrator needs to manage the autobooting scenarios. There are multiple scenarios where you can have this option enabled or disabled. For instance, during rollout to minimize the end user impact or during patch cycles to allow the patches to be installed and the reboots to <ul style="list-style-type: none"> <li data-bbox="483 541 1526 615">  If you enable this option, be aware that the McAfee Endpoint Encryption software does not protect the data on the drive when it is not in use. </li> </ul> </li> <li data-bbox="443 632 1526 688">• <b>Log on Message</b> — This could be an appropriate place to display your organization's legal disclaimer or any other appropriate messages. <ul style="list-style-type: none"> <li data-bbox="483 709 1526 751">  For a pilot phase, you can have your administrator or helpdesk phone number here. </li> </ul> </li> <li data-bbox="443 779 1526 806">• <b>Do not display previous user name at log on</b> — Leave this option checked (enabled).</li> <li data-bbox="443 827 1526 884">• <b>Enable on screen keyboard</b> — Leave this option checked (enabled), especially for tablets or on screen mouse device systems.</li> <li data-bbox="443 905 1526 1360">• <b>Add local domain users</b> <ul style="list-style-type: none"> <li data-bbox="483 940 1526 997">• <b>Disabled</b> — Selecting this option does not add any local domain users to the client system.</li> <li data-bbox="483 1018 1526 1199">• <b>Add all previous and current local domain users of the system</b> — This option adds the previously/ currently logged in domain users to the client system. If this is enabled, the EEAgent queries the system for the local users (who have the permission to logon to the localhost) who have logged on to the client. EEAgent then sends the collected data to the McAfee ePO server. The users are then added to EEPC users in ePolicy Orchestrator. (This works only with Active Directory)</li> <li data-bbox="483 1220 1526 1360">• <b>Only add currently logged on local domain user(s); activation is dependent on a successful user assignment</b> — Leave this option selected (enabled). On selecting this option, only the domain users who are logged on to the current Windows session, are added to the system and hence EEPC is activated, even if the administrator has not explicitly assigned the user to the client system. <ul style="list-style-type: none"> <li data-bbox="508 1381 1526 1476">  If you select this option, at least one user should be added to the client system for a successful EEPC activation on the client. The activation does not happen until a user logs on to Windows. </li> </ul> </li> </ul> </li> <li data-bbox="443 1497 1526 1591">• <b>Enable Accessibility</b> — Leave this option selected (enabled). This functionality allows visually impaired users to listen to voice as guidance when the user moves the cursor from one control to the next, in the Pre-Boot environment.</li> <li data-bbox="443 1612 1526 1759">• <b>Disable PBA when not synchronized</b> — Leave this option checked (enabled). When selecting this option, the user is blocked from logging on to PBA in the client system, if the client system is not synchronized with the ePolicy Orchestrator for the set number of days. In this case, to log on to the client system, you need to perform the Administrator (machine) recovery.</li> <li data-bbox="443 1780 1526 1898">• <b>Get username from token</b> — Leave this option checked (enabled). On selecting this option, the available user information on the client system, is automatically retrieved from the inserted smartcard; hence the Authentication window does not prompt for a username. The user can then authenticate just by typing the correct PIN.</li> </ul>

**Table 3-1 Recommended Product Settings Policies** *(continued)*

Policy Options	Recommendations
	<p>You need to enable the matching rules that are required for matching smartcard user principle name (UPN) with EEPC usernames.</p> <ul style="list-style-type: none"> <li>• <b>Enable SSO</b> — Leave this option checked (enabled).               <ul style="list-style-type: none"> <li>• <b>Must match user name</b> — Leave this option checked (enabled).</li> <li>• <b>Using smart card PIN</b> — Leave this option checked or unchecked based on whether the eToken/smart card is used or not.</li> <li>• <b>Synchronize Endpoint Encryption Password with Windows</b> — Leave this option checked (enabled).</li> <li>• <b>Allow user to cancel SSO</b> — Leave this option checked (enabled).</li> </ul> </li> <li>• <b>Require Endpoint Encryption logon</b> — Leave this option checked (enabled).</li> <li>• <b>Lock workstation when inactive</b> — Leave this option unchecked (disabled).</li> </ul>
<b>Recovery Tab</b>	<ul style="list-style-type: none"> <li>• <b>Enabled</b> — Leave this option checked (enabled). This is enabled by default to make sure that the recovery is possible at any stage of the EEPC management.</li> <li>• <b>Key size</b> — After consulting with your IT security, set the key size to the size adequate for your organization requirements. This refers to a recovery key size that creates a short Response Code for the recovery.</li> <li>• <b>Message</b> — You could use this option to display your helpdesk phone number or instruct the user to use the self recovery option.</li> <li>• <b>Allow user to update self-recovery answers</b> — Leave this option checked (enabled) only when required. On enabling this option, the client user's self-recovery details can be reset, then the user has to enroll the self-recovery details with new self-recovery answers.</li> </ul> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  <p>Before resetting the self-recovery questions on the client system, make sure that you have enabled the <b>Enable Self Recovery</b> option under <b>User Based Policy   Self-Recovery</b>. Only initialized users can reset their self-recovery details.</p> </div>
<b>Boot Options Tab</b>	<ul style="list-style-type: none"> <li>• <b>Enable Boot Manager</b> — Leave this option unchecked (disabled).</li> <li>• <b>Always enable Pre-Boot USB support</b> — Leave this option checked only when needed. (enabled). This USB audio functionality allows the visually challenged users to listen to an audio signal as a guidance when the user moves the focus from one field to the next using mouse or keyboard, in the Pre-Boot environment.</li> <li>• <b>Always enable Pre-Boot PCMCIA support</b> — Leave this option unchecked (disabled).</li> <li>• <b>Graphics mode</b> — Automatic.</li> </ul>
<b>Theme Tab</b>	<p>It is better to have the default option enabled as it is simple to deploy and manage.</p>
<b>Encryption Providers Tab</b>	<ul style="list-style-type: none"> <li>• <b>Use compatible MBR</b> — Leave this option unchecked (disabled).</li> <li>• <b>Fix OS boot record sides</b> — Leave this option unchecked (disabled).</li> <li>• <b>Use Windows system drive as boot drive</b> — Leave this option unchecked (disabled).</li> </ul>

---

## Recommended User-Based Policy Settings

The User-Based Policy controls the parameters for EEPC user accounts. For example, it contains the options for selecting a token type (including password and smartcard) and password content rules.

You can configure the User Based Policies by navigating through **Menu | Policy | Policy Catalog**, then selecting **Endpoint Encryption 1.2.0** from the Product drop-down list.

Select User Based Policies from the **Category** drop-down list. Locate the **My Default** policy and click **Edit Settings**. For more information about individual policy setting, see the *McAfee Endpoint Encryption - 6.2 (EEPC) and 1.1 (EEMac) Product Guide*.

### User Based Policies in EEPC 6.2


A requirement of EEPC 6.2 is that you need to specify which groups of users are allowed or not to use the Policy Assignment Rules. The allowed users get their required User Based Policies. Users that are not allowed to use the Policy Assignment Rules inherit the default User Based Policies assigned to the system.

Enforce the desired user-based policy to a user assigned to a client system by enabling the **Configure UBP enforcement** option.



It is always better to assign the User Based Policies at the system level or branch level if possible, rather than assigning using the Policy Assignment Rules. However, you can use the Policy Assignment Rule option, if required, for assigning different policies to different users.

**Table 3-2 Recommended User Based Policy Settings**

Policy Options	Recommendations
Authentication Tab	<ul style="list-style-type: none"> <li>• <b>Token type:</b> Select <b>Password only</b>. There are a number of other tokens that can be effectively used for your authentication as required. However, the Password only token is as strong as any other token that you could configure.</li> <li>• <b>Certificate rule</b> <ul style="list-style-type: none"> <li>• <b>Provide LDAP user certificate</b> — Leave this option checked (enabled).</li> <li>• <b>Use latest certificate</b> — Leave this option checked (enabled).</li> </ul> </li> </ul> <div style="border: 1px solid #ccc; background-color: #f0f0f0; padding: 5px; margin: 10px 0;">  The <b>Certificate rule</b> options are not active if <b>Password only</b> token is selected.         </div> <ul style="list-style-type: none"> <li>• <b>Logon hours</b> — You could enable and set the logon day and time-line as required. It is better to have this disabled if you do not have a specific requirement.</li> </ul>
Password Tab	<ul style="list-style-type: none"> <li>• <b>Change Default Password</b> — Leave this option unchecked (disabled) - This leaves the default password as 12345 for all new users. All new users are prompted to change the default password during user initialization.</li> <li>• <b>Password Change</b> — Disable all of these settings as you would be using SSO and don't want to cause conflict with Windows password requirements.             <ul style="list-style-type: none"> <li>• <b>Enable Password history</b> — Leave this option checked (enabled) to prevent users from reusing passwords unless your security policy exempts users from using new passwords.</li> <li>• <b>Prevent change</b> — Leave this option unchecked (disabled).                 <ul style="list-style-type: none"> <li>• <b>Require change after ___ days (1-366)</b>—Leave this option unchecked (disabled).                     <ul style="list-style-type: none"> <li>• <b>Warn user ___ days before password expiry (0-30)</b>—This is disabled by default when you disable the <b>Require change after ___ days (1-366)</b> option.</li> </ul> </li> </ul> </li> </ul> </li> <li>• <b>Incorrect Passwords</b> <ul style="list-style-type: none"> <li>• <b>Timeout password entry after ----invalid attempts (3-20)</b> — Set required number of password invalid attempts.</li> <li>• <b>Maximum disable time ----- minutes (1-64)</b> — This is disabled by default when you disable the <b>Timeout password</b> option.</li> <li>• <b>Invalidate password after ----- invalid attempts</b> — Leave this option checked (enabled).</li> </ul> </li> </ul>
Password Content Rules Tab	<ul style="list-style-type: none"> <li>• <b>Password length</b> — Use default.</li> <li>• <b>Enforce password content</b> — Use default.</li> <li>• <b>Password content restrictions</b> — Use default or enable restrictions for better password strength.</li> </ul>
Self-Recovery Tab	<ul style="list-style-type: none"> <li>• <b>Enable self-recovery</b> — Leave this option checked (enabled).</li> <li>• <b>Invalidate self recovery after No. of invalid attempts:</b> Enable and set the number of attempts to a number that does not abruptly lock out the Self Recovery.</li> <li>• <b>Questions to be answered</b> — Can be set to 3. This can give you the required security without giving the user a lot of pain of keying in the characters. However, it is up to the administrator to decide this number depending on the requirement.</li> <li>• <b>Logons before forcing user to set answers</b> — Set this to 0. This makes sure the users set the answers during the user initialization.</li> <li>• <b>Questions</b> — Use the default ones or configure the questions as required.</li> </ul>

## Phased deployment strategies

EEPC deployment (first time installation) can be done in various phases with different policy settings for different corporate environments. A model policy setting is explained in the recommended policy settings sections.

### Phased deployment (first time installation)

There can be a number of scenarios where the PBA creates challenges during the EEPC deployment. For a safe and smooth deployment and activation process, you can easily create different sets of EEPC system policies and do the deployment in various phases.

During the first time installation, it is a best practice to create the first set of policy settings with **Encryption** set to **None** and **Automatic Booting** enabled. You can create a second set of policy settings which enables the encryption and the PBA.



When the first set of policies is in use, the client systems are unprotected.

#### High level process

- After deploying the EEPC packages, create an EEPC system policy with the following settings:
  - Select the encryption option as **None** under **Encryption tab | Encrypt**.
  - Enable the **Enable Automatic Booting** option under **Log On tab | Endpoint Encryption**.
  - Enable **Add local domain users** option under **Log On tab | Endpoint Encryption**.
- Enforce this policy to the client systems. This activates EEPC, but encrypts no disks and requires no authentication.
- You can now configure the second set of policy with the required encryption option other than **None** and autobooting disabled.
- Use the automatic booting policy as the default. In this mode, the Add Local Domain Users feature captures all Windows domain accounts that access the system. These accounts are added as valid Pre-Boot enabled accounts to be used in the Pre-Boot environment.
- Create a query in ePolicy Orchestrator to find all systems that need to stop autobooting and assign the second policy to these systems.
- Send an agent wake-up call from ePolicy Orchestrator to apply the policy with Pre-Boot Authentication to all required systems.
- The systems will start with PBA as and when the new policy is received.

This phased deployment will temporarily enable automatic booting and then when the query is run, it enables the Pre-Boot Authentication policy. This ensures that EEPC gets activated when the system is in the field and ensures that the end user's account gets added as a valid Pre-Boot account before encrypting and activating PBA.

This kind of phased deployment can be very useful as and when the administrator meets with challenges such as patching cycles, re-imaging process, deploying product and managing other autoboot scenarios.



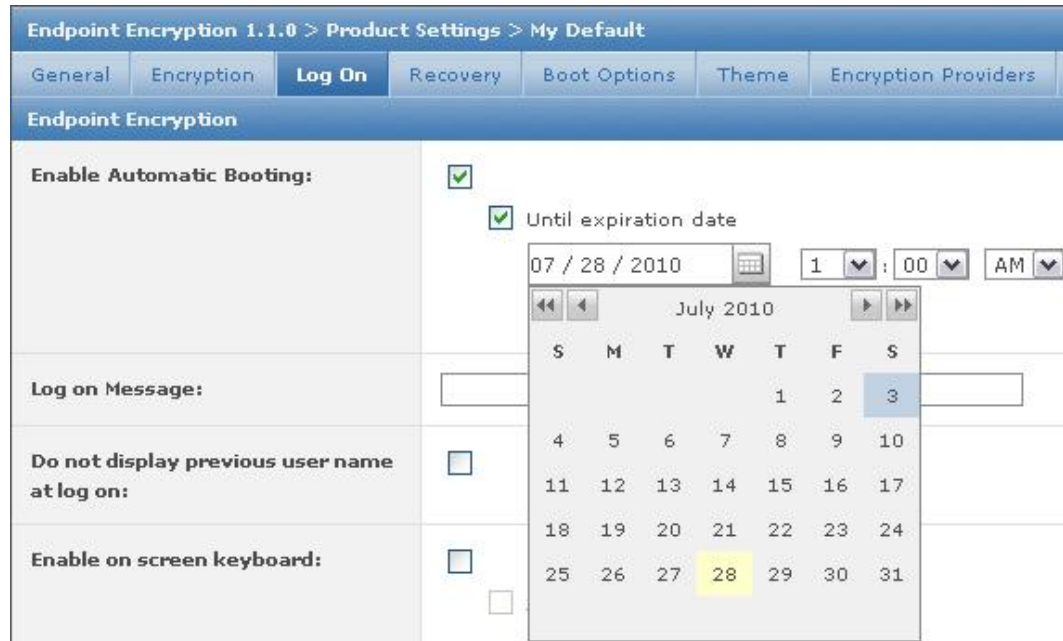
Perform phased deployment in batches of systems from the System Tree.



## Auto booting

Auto Booting (Enable Automatic Booting) is used by administrators for re-imaging process, patching cycles, and product deployments. Many software installation packages require one or more restarts of the target computer, and autobooting automatically authenticates without user or administrator intervention. The administrator can define a window of time-line during which autobooting remains active.

The autoboot feature terminates when the defined time-line window has elapsed.



**Figure 3-6 Configure auto booting**



Since this policy setting temporarily bypasses the normal logon process for EEPC installed systems, computers receiving this policy will be vulnerable while Autobooting remains active. To minimize the risk, make sure that you carefully review the inclusive dates and times that Autobooting remains active before deploying this policy.



# 4

## Deployment and activation

The purpose of this section is to provide guidance with troubleshooting on why the Windows operating system will not start; encrypted systems do not allow access to the operating system until PBA is completed.

Administrators should be mindful that fixing certain Windows problems on an encrypted system may require extra caution in the event that the registry must be edited or a driver should be modified.

Traditional recovery procedures will also change on a system encrypted with EEPC 6.2. For example, the entire disk is encrypted which means the file systems and disks are accessible only when the Pre-Boot authentication is complete.

The EETech User Guide provides instructions on how to create a customized pre-installation disk (EETech Windows PE V1 and V3) with the EEPC drivers loaded. This disk allows the administrator to access an encrypted hard drive or Opal drive to update the drivers or the registry. For more information, refer to the KnowledgeBase article <https://kc.mcafee.com/corporate/index?page=content&id=KB75034>.

### **Booting the EEPC installed client requires the physical presence of the client user to supply credentials at the EEPC PBA page.**

To gain access to an encrypted computer, the user must always enter credentials at the PBA screen. It is important that this change in client operation be understood and adopted into your operating procedures. Administrators should be mindful of dispatching drivers/service packs to client systems as the system will inevitably require reboot after install.

The **Enable Automatic Booting** option in the **Product Settings Policy** allows access to the EEPC installed systems without actually having to authenticate through PBA. However, it is the administrators' responsibility to ensure that system security is not compromised if this option is selected, as Autoboot effectively removes system security. Alternatively, you can also use the OS refresh process to keep the systems secure with minimal user intervention.

### **Contents**

- ▶ *Basic preparations and recommendations*
- ▶ *High level process of the installation*
- ▶ *Client task to deploy the EEAgent and EEPC packages*
- ▶ *Add group users*
- ▶ *EEPC activation sequence*
- ▶ *Activate EEPC using Add local domain users*

## Basic preparations and recommendations

The following recommendations will make sure that your data is protected during and after the encryption process.

### As with any roll out and deployment, it is advisable to back up the system before you encrypt it, and perform regular backups

It is good practice to back up the system before installing EEPC to ensure data is not lost in the unlikely event a problem occurs. The EETech recovery tools can also be used to decrypt and recover any unbootable disks. Please refer to the EETech User Guide for more information.



When upgrading EEPC the Mfееpehost service must not be stopped either manually or by third party software since this can cause problems. Also note that during an upgrade the system must be kept powered on until the software (both Host and Admin portions) complete installing.

### CHKDSK /r Clean up the disk before you encrypt it

Hard disks that are damaged, or have a high number of undiscovered bad sectors, may fail during the full disk encryption process. Run a **CHKDSK /r** command prior to installing EEPC to make sure the disk is healthy. Optionally, run the OEM diagnostic tools to make sure that all other HW components are working correctly.

### Understand the supported tokens/readers for EEPC

Make sure that the supported reader drivers are installed in your client system before trying to install Endpoint Encryption for PC. Make sure to obtain the correct drivers from the manufacturer website and review their release notes to avoid any known issues with the tokens or readers. The supported tokens and readers are listed in these KB articles:

- Supported Readers used for authentication in McAfee Endpoint Encryption for PC 6.x: <https://kc.mcafee.com/corporate/index?page=content&id=KB71554>
- Supported Tokens used for authentication in McAfee Endpoint Encryption for PC 6.x: <https://kc.mcafee.com/corporate/index?page=content&id=KB71555>

### Maintain separate test and production clients

Enterprise administrators are advised to maintain separate test and production environments. Modification to the production server should be limited. Use the test system to test software updates, driver updates and Windows Service Packs prior to updating the production systems.

### Build and test recovery tools

The administrator needs to be aware that there will be changes to the normal client boot process due to installing EEPC. Administrators are advised to:

- Create and test the customized EETech WinPE V1 or V3 Disk with EEPC drivers installed.
- Create and test an EETech Standalone Boot disk.

### Run a pilot test of software compatibility

We recommend that you run a pilot test of EEPC on a client system. This will make sure that EEPC is not in conflict with any encryption software on the client computers before rolling out to a large number of clients. EEGO can be a valuable tool to detect the presence of third party encryption software that may prevent activation or create further issues with EEPC.

This is particularly useful in environments that use a standardized client image.

Administrators should also run performance testing during the pilot test.

McAfee professionals did not come across any performance related issues with EEPC during our own testing, however, this may vary depending upon the processor, memory, and drivers.

### Do a phased deployment

An occasion may arise when the PBA creates challenges during deployment. For a successful deployment and activation, you can create a different set of EEPC system policies and deploy in phases enabling the **None** option under **Encrypt** and **Enable Automatic Booting** option under **Log on** tab. Create deployment tasks and deploy EEPC to systems arranged in groups or batches in the **System Tree**. You can also base it on a specific tag in ePolicy Orchestrator.

### Add user to the client system

You should add at least one user to the client system for EEPC to activate on the client.

### Perform disk recovery on decrypted disks

Wherever possible, as a best practice, if you need to perform any disk recovery activities on a disk protected with McAfee EEPC, we recommend that you first decrypt the disk. For more information about decrypting the EEPC installed system, see *McAfee Endpoint Encryption - 6.2 (EEPC) and 1.1 (EEMac) Product Guide* and the *McAfee EETech User Guide*.

### Educate the client user with the Password/Token/PIN secrecy

Educate your client users to understand they are responsible for the security of their password, PIN, or token details. Encourage them to change their password, or request a new PIN, if they feel that it may have been compromised.

### Make sure password strength is sufficient

Make sure that your password policy is strong enough for your requirements.

---

## High level process of the installation

This section lists the steps and considerations involved in EEPC deployment and activation.

This procedure is explained in more detail in the *McAfee Endpoint Encryption - 6.2 (EEPC) and 1.1 (EEMac) Product Guide* and the *McAfee Endpoint Encryption for PC 6.2 Quick Start Guide*.

### Task

- 1 Install the EEPC extensions into ePolicy Orchestrator 4.5 Patch 4 Hotfix 1 or later. Check for the correct and latest version of the extension. Install EEAdmin extension first then EEPC.
- 2 Check in the EEPC packages to ePolicy Orchestrator 4.5 Patch 4 Hotfix 1 or later. Check for the correct and latest version of the EEAdmin and EEPC packages.
- 3 Register your LDAP Server. Check for the correct domain and Server IP address of your LDAP server configured.
- 4 Create **EE LDAP Server User/Group Synchronization** task and schedule it to run. Check for the correct format of the user attributes while scheduling the task.
- 5 Modify the Product Settings and User-Based Policies, as appropriate. Plan and verify the policy settings for your organization's requirements.

**Deployment and activation**

Client task to deploy the EEAgent and EEPC packages

- 6 Add a user to the client system. Decide whether to add the users manually in ePolicy Orchestrator or to add users using the **Add local domain user** option present under the **Product Settings Policy**. At least one user must be assigned to each client in order to activate EEPC on it.
- 7 Create a client task to deploy the EEPC components to the client systems. Make sure that you deploy the packages in the right order (EEAgent then EEPC).
- 8 Test for successful deployment, activation and encryption on targeted endpoints. Make sure to make use of the reporting facilities available in the ePolicy Orchestrator management software.

## Client task to deploy the EEAgent and EEPC packages

We recommend that you create a new system group in ePolicy Orchestrator for EEPC deployment. Name it EEPC Test Systems or EEPC Production Systems, respectively, for example.

Do not create the deployment task at the **My Organization** level of the **System Tree**. Select a group in the **System Tree**, go to the **Client Tasks** tab and create the deployment task.

### Importing systems from Active Directory to ePolicy Orchestrator

McAfee ePO provides an **AD Synchronization/NT domain** task to synchronize ePolicy Orchestrator with the configured Active Directory. This option allows you to map the ePolicy Orchestrator **System Tree** structure with a registered AD. Using this option, you can import and effectively manage large numbers of systems in ePolicy Orchestrator.



This option works only with Active Directory.

Refer to the ePolicy Orchestrator product documentation for versions 4.5 and 4.6, for detailed procedures on how to import systems from Active Directory to ePolicy Orchestrator.

### Order of the EEAgent and EEPC deployment

It is not mandatory to have two different tasks for the product deployment. You can create one single task to deploy both packages, but don't forget that they need to be deployed in the right order. The EEAgent package should be followed by the EEPC package.

If you configure to deploy the EEPC package followed by the EEAgent package then the client system restarts in the middle as required and the EEAgent would never get deployed.

So, it is always better to execute the deployment using a single task wherein you need to deploy the EEAgent package first then the EEPC package.

The screenshot shows the 'Client Task Builder' interface in the 'Configuration' step. The 'Target platforms' section has 'Windows' selected. The 'Products and components' section lists two packages: 'Endpoint Encryption Agent for Windows 1.1.0.20' and 'Endpoint Encryption for PC 6.1.0.20'. Both are set to 'Install' action, 'Language Neutral' language, and 'Current' branch. The 'Options' section has 'Run at every policy enforcement (Windows only)' unchecked.

**Figure 4-1** EEAgent and EEPC packages deployment

You can also create two separate tasks to deploy the packages, providing you wait for the first deployment (EEAgent) to complete before deploying the second package. You can also verify the completion of the EEAgent deployment, before deploying the EEPC package, by creating and executing a customized query from the McAfee ePO server. If the EEPC package is deployed first, you can run the EEAgent task and deploy it later.

### End user experience

The deployment task pushes both the Endpoint Encryption Agent and the EEPC components to the selected systems. The installation is silent, however, the user is prompted to restart the client when the EEPC component install is complete. It is important that the user restarts the client PC when prompted. If this does not happen, EEPC will not activate.

---

## Add group users

Group Users are the EEPC user accounts that are allocated to every encrypted system. They are typically administration accounts used for troubleshooting and supporting the client in a given group.



If you choose to add a Group or an Organizational Unit (OU), you will not see the individual user names. Instead, you will see the entire Domain Name of the Group or Organizational unit.

All EEPC user accounts, including Group User, accounts get assigned the default password upon creation. If the default password is not changed in the User-Based Policies then use **12345** as the default password for the first time you log on with these user accounts.

If you want the system to capture the user's credentials automatically without having to make them use a default password on PBA, enable the **Do not Prompt for default password** option under **User Based Policies | Password**.

### Users

To access the data on an encrypted computer, the user must go through the PBA. If the **Enable Auto Booting** option is not enabled then the client user is presented with the PBA screen when the system is restarted after activating EEPC.

During the first Pre-Boot after activation, the user needs to initialize the user account with the default password and enroll for the self recovery if this feature has been enabled in the policy.

During the initialization process, users will set up their Pre-Boot credentials to unlock the disk. Only the assigned users from a registered LDAP server will be accepted by EEPC PBA.



At least one EEPC user is required to be assigned to EEPC on each client; this could be an administrative user.

### Add local domain users

This option automatically adds the previously logged in domain users to the client system, so that administrators don't have to manually assign users to the client systems in the ePolicy Orchestrator console.

This option can be enabled as and when needed through the Endpoint Encryption Product Settings Policies (**Menu | Policy | Policy Catalog | Endpoint Encryption 1.2.0 (Product Settings) | Log on tab | Add local domain users**).

When enabled, the EEAgent queries the client system for the currently/previously logged on domain users to the client. The EEAgent will then send the collected data to the McAfee ePO server. These users will then be assigned to the client system.



We recommend that you have this option enabled, so that you will always be able to authenticate to the Pre-Boot of the client without having to manually assign the users to the client system in the ePolicy Orchestrator console. However, this is a responsibility of the administrator to decide whether this is required or not depending on corporate requirements.

## Prerequisites

The following prerequisites are required to add the local domain users to the Endpoint Encryption client systems:

- McAfee Agent 4.5 Patch 1 or later is deployed.
- McAfee **EEAgent for Windows** package is deployed to the required client systems.
- McAfee **Endpoint Encryption for PC** package is deployed to the required client systems.
- Registered Active Directory is added and configured correctly.



The **Add local domain users** option is supported with Active Directory only.

- An automated **EE LDAP Server User/Group Synchronization** task should be scheduled and run.
  - This task is used to map Active Directory attributes to the Endpoint Encryption settings. This is required for every Registered LDAP server that is to be used with Endpoint Encryption.
- Client systems should be using Active Directory for authentication.
  - These domain users must be previously or currently logged in users.

## At the client side

The **Add local domain user** option is processed during the next agent to server communication. If this option is enabled in the policy settings, the EEAgent queries the client system for the domain users who have logged on to the client. The EEAgent will then send the collected data to the McAfee ePO server.

The data that is transmitted back will be a list of user names and the domain names. Local Domain users are detected by examining the Windows registry which has the profile list. This list provides the list of users who have logged in to the system.

## At the server side

When the EE Admin receives a message for adding local domain users, it executes the following steps.

- It attempts to find the domain name that the user belongs to. This is done by querying the Registered Active Directory that is configured with the automated **EE LDAP Server User/Group Synchronization** task.
- If a registered LDAP server is found then it matches the domain name of the user. An LDAP query is performed and attempts to find an LDAP node with a **samaccountname** that matches the user name.

If the user name is found then it will be assigned to the corresponding client system. You can query the added users by using the **View Users** option under **Menu | Data Protection | Encryption Users | Actions | Endpoint Encryption | View Users**.



## EEPC activation sequence

When EEAgent and EEPC are successfully deployed, the users will be prompted to restart their system.



The restart can be canceled, however, EEPC will not become active on the client until the restart has occurred. Therefore, the restart is essential for activation of EEPC on the client to proceed.

### Endpoint Encryption Status

System restarts as initiated. You will not yet see the PBA page as the EEPC software is not yet active on the client. However, you should now be able to see the new option **Quick Settings | Show Endpoint Encryption Status** in the McAfee System Tray icon.

### EEAgent synchronization with the McAfee ePO server

The status in the **Show Endpoint Encryption Status** window will show as **Inactive** until EEAgent synchronizes with the McAfee ePO server and gets all the users assigned to it. This is referred to as an ASCII event.

It can be manually triggered on the client by opening the **McAfee Agent Status Monitor** and clicking **Collect and Send Props**. It can also be triggered from the McAfee ePO server by doing an agent wake-up call, otherwise, you will need to wait for the scheduled agent -server communication interval to occur (the default is 60 minutes). After two agent-server communication intervals the status, EEPC activation will begin. The activation process requires a number of McAfee ePO events to be sent, and this can take some minutes to occur. Once the client-server communication has completed, the Endpoint Encryption Status will switch to **Active** and encryption will start based on the policy defined.



During activation, hibernation cannot be used. It is recommended that hibernation is disabled through Active Directory Group Policy while the rollout is in progress.

### User intervention during encryption

The user can continue to work on the client system as normal even during encryption. Once the entire disk is encrypted, the technology will be completely transparent to the end user.



It is safe and risk-free to restart the client system during encryption.

### PBA

When the client system is restarted and EEPC is first activated, the user should log on with the username that matches the user attribute set in the **EE LDAP Server User/Group Synchronization** task and the default password of **12345** (this is the McAfee default password which can be changed in the User Based Policy) in the PBA page. The user is then prompted to change this password and enroll for self-recovery based on the policy set.

If you want the system to capture the user's credentials automatically without having to make them use a default password on PBA, enable the **Do not prompt for default password** option under **User Based Policies | Password**.



We recommend that you change the default password and enforce policies with stronger passwords.

### Single Sign On (SSO)

The system then boots to Windows. This first boot establishes SSO (if it has been enabled). On future restarts, the user will login to PBA only. Once authenticated, SSO will auto-login to Windows.

In short, the SSO option facilitates the user with the single authentication to the Operating System even when PBA is enabled. Though it requires an extra step, disabling SSO is the more secure configuration.



When the **Must match username** option is enabled, both the EEPC user name and the Windows user name should match for SSO to work, regardless of which domain the user is part of. This user can even be a local user.

When the **Synchronize Endpoint Encryption password with Windows** option is enabled, the EEPC password is reset to the Windows password, however, be aware if the **Password history** option is enabled, and the EEPC password is same as the Windows password, then synchronization will not occur.



On changing the EEPC password, the synchronization will not be reset. Synchronization of the password will occur only when there is a change in the Windows password.

---

## Activate EEPC using Add local domain users

Using the **Add local domain users** option, you can activate EEPC on the client systems without manually adding users in ePolicy Orchestrator.

Make sure that at least one manually added user is assigned to the client system. For example, this could be an admin user assigned to all systems.

### Task

- 1 Configure the **Product Settings Policy** with **Add local domain users** option enabled.
- 2 Log on to the client system. After the agent to server communication interval, the **Add local domain users** option adds the previously/currently logged on domain users to the client system.
- 3 EEPC is activated in the client system during the next ASCII. You can now restart the client to log on using the PBA page.



This option provides automatic user assignment, which helps the administrators in not having to manually assign users to client systems in the McAfee ePO console. The recommended best practice is to manually assign at least one user to all systems to ensure that EEPC activation happens successfully even if the **Add local domain user** option fails to function as configured. However, if this option is configured correctly, it will not fail. A general recommendation would be to manually add a group of support users to all systems, then activate EEPC using the **Add local domain users** option. You can remove these users at a later stage after completing the deployment.

# 5

## Operations and maintenance

Managing your systems in different batches, branches or groups will make a great impact for EEPC deployment. It is a good practice to arrange the systems in ePolicy Orchestrator in department level or batch level, then deploy the product to these batches one by one.

### Managing the servers and client systems

Client deployment in batches with an appreciable number of systems is a good practice by itself.

Please keep the following recommendations in mind while managing the servers and client systems:

- Do not try to create the EEPC deployment task at the root level of your system tree and activate it. It is a good practice to deploy EEPC to the systems at the sub-level branches.
- Do not deploy EEPC to the server systems, specially the server hosting your McAfee ePO server.
- Secure your McAfee ePO server and database system in the most secured location and keep it accessible for authorized personnel only.

### Contents

- *How does disabling/deleting a user in Active Directory affect the EEPC user*
- *Manage Machine Keys*
- *Configure role based access control for managing EEPC*
- *EEPC 6.2 scalability*

---

## How does disabling/deleting a user in Active Directory affect the EEPC user

Every user account has an objectGUID in LDAP and an entryUUID in Open LDAP. If a user account is deleted from LDAP and another is created with the same user name, this new user account will be a different entity. This is because the objectGUID would have changed for the new user.

### To delete a user in LDAP

You must first delete the user in LDAP, then run the **EE LDAP Server User/Group Synchronization** task and send an Agent wake-up call. The user will disappear from EE Users list after the **EE LDAP Server User/Group Synchronization** task is complete.

The ePO Server Setting option **If user is disabled in LDAP server** within **Server Settings | Edit | General** can be configured to disable, delete, or ignore the user if the user has been disabled in the LDAP Server.

### What if a user is disabled from LDAP?

If a user account that is initialized on the client system, and is later removed from LDAP, then it will be automatically deleted/ignored from the client when the next EE LDAP User/Group Synchronization task runs. To authenticate through the client PBA with a disabled or deleted LDAP user name, you should once again add the user to the LDAP and initialize the same user name on the client with the default password.

This does not remove the users from the EEUsers list in ePolicy Orchestrator, however, it removes/deletes/ignores the users from the client system based on the option set in the Server Settings.

### Is it possible to just disable the EEPC user when removed from LDAP?

It is not possible to disable an EEPC user when it has been removed from LDAP. The user is removed from the EE Users list if deleted in LDAP during the next **EE LDAP Server User/Group Synchronization** task.

### What if the EEPC user assignment is deleted/removed?

If the EEPC user assignment is deleted from a system, the user might still be assigned back to the client system if the **Add local domain users** option is enabled in the **Product Settings Policy**. For this to work, the user must have logged on to Windows at least once and the domain to which client system is connected should have been registered in ePolicy Orchestrator. You can also manually add users using **Add EE: Users** option in ePolicy Orchestrator.

---

## Manage Machine Keys

The purpose of encrypting the client's data is to control access to the data by controlling access to the encryption keys. It is important that keys are not accessible to users.

The key that encrypts the hard disk sectors needs to be protected. These keys are referred to as Machine Keys. Each system has its own unique Machine Key. The Machine Key is stored in ePolicy Orchestrator database to be used for client recovery when required.



For more information about reusing machine keys, refer to the KnowledgeBase article <https://kc.mcafee.com/corporate/index?page=content&id=KB71839>.

### Machine Key re-use

Machine key re-use option is used to activate the system with the existing key present in the McAfee ePO server. This option is highly useful when a boot disk gets corrupted and the user cannot access the system. The boot disk corrupted system's disks other than the boot disks can be recovered by activating it with the same key from McAfee ePO.



Machine key re-use is not applicable to systems having self-encrypting (Opal) drives.

### What happens to Machine Keys when an EEPC-active system is re-imaged?

All existing data of the system is lost and hence the machine Key is lost when an EEPC-active system is re-imaged.

### What happens to the Machine Key when you delete an EEPC-active system from ePolicy Orchestrator?

The Machine Key remains in the ePolicy Orchestrator database; however, the key association with the client system is lost when the client system is deleted from ePolicy Orchestrator. When the client system reports back to ePolicy Orchestrator during the next ASCI, it will appear as a new node. A new

node does not have any users assigned to the client system. The administrator must therefore assign users to allow login, or enable the **Add local domain user** option in the **Product Setting Policy**. Also, the administrator must configure the required policies in ePolicy Orchestrator.

The next data channel communication after adding the users and configuring the policies will make sure:

- The Machine Key is re-associated with the client system and the recovery key is available.  
When the associated Machine Key is not present with the new node, ePolicy Orchestrator sends a Machine Key request. If the user is logged on to the client system, an agent to server communication between the client and the McAfee ePO server ensures the Machine Key is updated in ePolicy Orchestrator and the users are updated on the client. Thereafter, the Machine Key will be available and admin recovery and policy enforcement will work.
- The users are assigned to the client system. Therefore, these users can straightaway log on to the client system.

You cannot log on to the client system before a proper agent to server communication occurs. In this situation, the re-association of the Machine Key can be performed using EETools . The recovery key will also be available; this can be used with the EETech tool to recover the client system.

For EETool details and procedures, refer to the HotFix Release Notes (Readme\_HF 582699).

### What happens to Machine Keys when transferring a client system from one McAfee ePO server to another?

The Machine Key remains in the ePolicy Orchestrator database, however, the key association with the client system is lost when the client system is transferred from another McAfee ePO server.

When a transferred client system reports back to ePolicy Orchestrator during the next ASCI, it will appear as a new node and will therefore not have any users assigned to it. The administrator must assign users to allow login, or, enable the **Add local domain user** option in the **Product Setting Policy**. The administrator must also configure the required policies in ePolicy Orchestrator.



To transfer all systems between McAfee ePO servers, the best process is to follow the ePO Disaster Recovery process. For more information, refer to the KnowledgeBase article <https://kc.mcafee.com/corporate/index?page=content&id=KB66616>.

The next data channel communication after adding the users and configuring the policies will ensure:

- The Machine Key is re-associated with the client system and the recovery key is available.  
When the associated Machine Key is not present with the new node, ePolicy Orchestrator sends a Machine Key request. If the user is logged on to the client system, an agent to server communication between the client and the McAfee ePO server ensures the Machine Key is updated in ePolicy Orchestrator and the users are updated on the client. Thereafter, the Machine Key will be available and admin recovery and policy enforcement will work.
- The users are assigned to the client system. Therefore, these users can straight away log on to the client system.

You cannot log on to the client system before a proper agent to server communication occurs. In this situation, the re-association of the Machine Key can be performed using EETools . The recovery key will also be available; this can be used with the EETech tool to recover the client system.

For EETool details and procedures, refer to the HotFix Release Notes (Readme\_HF 582699).



To export old machine (dissociated) keys from McAfee ePO 4.5 use EETools, and from McAfee ePO 4.6 use the ePO Scripting API.

### What happens to Machine Keys when moving systems from one branch to another in ePolicy Orchestrator?

The LeafNode is not deleted from ePolicy Orchestrator database when a system is moved from one branch to another in ePolicy Orchestrator, hence the Machine Key is available for the particular client system.

### How to destroy the recovery information for an EEPC installed system?

When you want to secure-erase the drives in your EEPC installed system, remove all users from the system (including those inherited from parent branches in the system tree). This will result in making the disks inaccessible through normal authentication as there are no longer any users assigned to the system. You need to then destroy the recovery information for the system using the option **Menu | Systems | System Tree | Systems tab | Actions | Endpoint Encryption | Destroy All Recovery Information** in the ePolicy Orchestrator console. This means that the system can never be recovered.

---

## Configure role based access control for managing EEPC

The ePolicy Orchestrator administrator rights management determines what administrators can perform while managing the Endpoint Encryption software.

The administrator can set up Endpoint Encryption specific permission sets to different users in ePolicy Orchestrator. The permission sets can be created for Executive Reviewer, Global Reviewer, Group Admin, and Group Reviewer. The Endpoint Encryption Administrator extension (EEADMIN.ZIP) enables ePolicy Orchestrator administrators to control Endpoint Encryption Systems that are managed through ePolicy Orchestrator.

The McAfee ePO administrator for EEPC is able to:

- Manage Endpoint Encryption users, policies and server settings
- Run queries to view the encryption status of the client systems
- View client system audits
- View McAfee user audits
- Manage Endpoint Encryption Providers

Administrative roles can be configured and implemented using the **Endpoint Encryption Permission Sets** option present in ePolicy Orchestrator. It is possible to configure a number of admin roles using this option. For example, you can create admin roles such as:

- **Endpoint Encryption Administrator:** User accounts in this level have full control of EEPC, but cannot manage any other software in ePolicy Orchestrator.
- **Endpoint Encryption Helpdesk:** User accounts in this level can do EEPC password resets only.
- **Endpoint Encryption Engineer:** User accounts in this level can do password resets as well as export recovery files to be used with EE Tech tool.
- **Endpoint Encryption Auditor:** User accounts in this level can view EEPC reports only.

Before you begin

- Make sure that your LDAP server is configured and registered in ePolicy Orchestrator.
- Make sure that you schedule and run the EE LDAP Server User/Group Synchronization task.
- Make sure that you enable the **Active Directory User Login** option in ePolicy Orchestrator. To enable, navigate through **Menu | Configuration | Server Settings | Active Directory User Login | Edit**, then enable **Allow Active Directory users to login if they have at least one permission set** option.

You can create different permission roles and assign them with different **Endpoint Encryption Permission Sets** to different users.

Edit Permission Set Group Reviewer : Endpoint Encryption	
<b>Policy Options</b>	<input checked="" type="radio"/> No permissions <input type="radio"/> View policy settings <input type="radio"/> Change and view policy settings
<b>User Management</b>	<input checked="" type="radio"/> No permission to user management <input type="radio"/> View user management <input type="radio"/> Change and view user management <input type="checkbox"/> Allow import of v5 users <input type="checkbox"/> Allow configuration of UBP enforcement
<b>Recovery Options</b>	<input type="checkbox"/> Allow clear SSO <input type="checkbox"/> Allow force user password change <input type="checkbox"/> Allow reset token <input type="checkbox"/> Allow viewing of user recovery information <input type="checkbox"/> Allow administrator recovery <input type="checkbox"/> Allow export of machine recovery information <input type="checkbox"/> Allow machine key re-use
<b>Query Options</b>	<input type="checkbox"/> Allow deletion of migration log items <input type="checkbox"/> Allow deletion of migration cache items <input type="checkbox"/> Allow deletion of v5 audit items

**Figure 5-1 Endpoint Encryption permission sets**

To verify the configured permission sets, log off from ePolicy Orchestrator, then log on with a user account that belongs to any one of the new roles.



Use correct format of the user name (domain\username) when logging on to ePolicy Orchestrator.

## EEPC 6.2 scalability

Use these configurations, recommendations on components, and considerations for scalability.

- ePolicy Orchestrator 4.5 Patch 4 Hotfix 1 and later
- EEPC 6.2

These considerations and settings will help improve scalability:

- Longer ASCII interval
- Password only deployments should remove certificate query from **EE LDAP User/Group Synchronization** task.



The User Certificate attribute is used by the McAfee ePO server to determine which certificate should be sent from McAfee ePO to the client, for example, for smartcard tokens. It is better not to query this attribute when you use the Password only token as tests have shown that LDAP query performance decreases when certificates are included in the query. Setting this attribute can also accumulate a large size of data in the database; therefore, you can remove the certificate query from **EE LDAP Server User/Group Synchronization** while using the Password only token.

- Phased rollout during migration, upgrade, or first time installation of EEPC 6.2.

These configurations and factors will degrade scalability:

- **Policy Assignment Rules** — The policy assignment rules should be setup in a logical order to ensure minimal processing. Create an ordered list of rules associated with a User Based Policy. For each user, the rules engine evaluates the rules in order, and the first rule that is satisfied defines which UBP is assigned to the user.



Make sure that you enable the Policy Assignment Rules for a small number of users to minimize overloading ePolicy Orchestrator.

Given that ePolicy Orchestrator needs to send all users down to a client during activation, each user will need to have rules run to associate a UBP with them (if UBPs are enabled and rules are defined). With **r** rules, **m** machines and **u** users, the worst case scenario would be an  $O[n^3]$  calculation ( $r * m * u$ ), which is not recommended.

Best practice is therefore to configure the rules in the correct order, such that they are defined in descending order of the number of users that each rule would “catch”. For example, if rule A catches 10% of users, rule B catches 80% of users, C 5%, D 2%, E 3%, the most efficient way of ordering the rules would be B->A->C->E->D, if the logic of your rules allows this to be done.

- Large number of user per machine (>20)
- Deployment of unnecessary languages (recovery questions)

The rate of activation can be calculated with the formula,  $N_{max} = ASCII_{secs} / M_{upstream} \cdot DC_{rate}$

Where,

- $DC_{rate}$  depends on hardware configuration of ePolicy Orchestrator and Database
- $M_{upstream}$  is the number of data channels (two) being sent from each client

For more details on EEPC 6.2 scalability, refer to the KB article <https://kc.mcafee.com/corporate/index?page=content&id=KB71363>.



# 6

## Migration and upgrade

EEPC 6.2 has an improved architecture and interface.

Due to these improvements, some functionality from earlier versions of the product is now handled differently.

### Contents

- ▶ *Best practices for migration and upgrade*
- ▶ *Export user assignments from 5.x.x database*
- ▶ *Import user assignments to McAfee ePO*
- ▶ *Upgrade to EEPC 6.2*

---

## Best practices for migration and upgrade

The information in this section helps you to understand the best practices and prerequisites for EEPC migration and upgrade that involve the following tasks. The detailed procedures to perform the following tasks are given in the *Endpoint Encryption for PC 6.2 Migration Guide*.

- Migrating user assignments from the 5.x.x database to the McAfee ePO server
- Exporting from 5.x.x database
- Importing the export file (the user information) into the McAfee ePO server that has EEPC 6.2
- Exporting audit information
- Importing audit information
- Upgrading the client system from EEPC 5.x.x
- Upgrading the client system from EEPC 6.x

### Migration tool

Make sure that you have the latest **EEMigration.ZIP** file of EEPC 6.2 to implement and perform the export. We recommend that you copy and extract the **EEMigration.ZIP** file to the folder where **Endpoint Encryption Manager** (EEM) is installed.

### Exporting 5.x.x database

- Make sure that you have access rights to view system and user properties on Endpoint Encryption Manager and the McAfee ePO server.

## Importing the systems or users from 5.x.x database into the McAfee ePO server

- Make sure that 5.x.x and 6.2 are connected to the same LDAP server during the export and import process.
- Make sure that you have registered an LDAP server on the McAfee ePO server before initiating the import process.
- Make sure that you have scheduled and run the **EE LDAP Server User/Group Synchronization Server** task before initiating the import process.
- Analyze the color-coordinated results in different phases of the import. It guides you to make appropriate decisions before proceeding to the next step.
- Do not navigate away or shut the browser when the import is running on ePolicy Orchestrator. Doing so interrupts the import thread and stops the import process. When the import is running, you can see the message **Please wait, assigning users to systems** in the top left of the McAfee ePO console.
- After you import the systems or users from 5.x.x database into the McAfee ePO server, check that the systems, users, and the audit details are imported as you expected. Check that the password token, self recovery, SSO details, if available, are imported as you expected.
- Conduct a policy review after the import process. If you need your 5.x.x policy settings for 6.2, you must set them before upgrading the client. Make sure that you enable the Encrypt product setting policy under **Endpoint Encryption 1.2.0 | Product Settings | Encrypt**. If this is not set, encrypted client system starts decrypting by default.



To initiate the encryption on the client, you must select any one of the options other than **None**. The default option **None** does not initiate the encryption.



Some firewall software enforce HTTP session timeouts. During the import you should review your firewall settings according to the manufacturer documentation and take the necessary actions to prevent the firewall from timing out the session.

- Before upgrading the client, make sure that the user's UBP enforcement settings are correct and the appropriate Policy Assignment Rule is created on McAfee ePO if those users are intended to use the non-default UBP.

## Upgrading to EEPC 6.2

- Make sure that the system to be migrated is managed by the McAfee ePO server.
- Migration of users directly from 5.x.x client to the new 6.2 client is not supported. Any migration of user assignments must be done on ePolicy Orchestrator before or after deploying EEPC 6.2 to the client system.
- To upgrade the client, first install the EEAgent, then the EEPC software packages.
- If 5.x.x users are found in the assigned LDAP OU/Group, the 5.x.x password token, SSO and Self Recovery data will be transferred to 6.2. If new users are present in the assigned LDAP OU/Group, then they are added to 6.2, as users not being initialized.

## General recommendations

- Retain the 5.x.x database for some time, so that you can access it case any loss or theft of a device after the migration.
- Migrate only a small number of systems as an initial test before doing a large-scale migration.
- If you are using the \$autoboot\$ user id in 5.x.x to boot your systems without actually having to authenticate through the PBA, then please be advised that the same option is now a feature in 6.2. So, make sure that you enable this policy feature (**Menu | Policy | Policy Catalog | Endpoint Encryption 1.2.0 | Product Settings | Logon | Enable Automatic Booting and Add local domain users**) to activate **Autoboot** while migrating the users and systems from 5.x.x to 6.2.



The Enable Automatic Booting option in the Product Setting Policy allows access to the EEPC installed systems without actually having to authenticate through PBA. However, it is the administrators' responsibility to ensure that system security is not compromised if this option is selected.

If you enable this option, be aware that the McAfee Endpoint Encryption software doesn't protect the data on the drive when it is not in use.

---

## Export user assignments from 5.x.x database

The export tool provided with EEPC allows the administrator to export the user assignments from 5.x.x database. The purpose of exporting the user assignments is to reduce the amount of configuration required by the administrator to upgrade from 5.x.x to 6.2.

The export output is a .ZIP file, which can be imported into the McAfee ePO server. The import process uses an import wizard on the McAfee ePO server after installing the applicable EE extensions.



The purpose of exporting systems from 5.x.x database is to export the user assignments. Migration export is not required if you do not want to migrate the user assignments.

## Best practices

- Make sure that you have the latest **EEMigration.ZIP** file from the EEPC 6.2 release package to implement and perform the export from 5.x.x Endpoint Encryption Manager.
- We recommend that you copy and extract the **EEMigration.ZIP** file to the folder where Endpoint Encryption Manager is installed.
- Make sure that you have the access rights to view system and user properties on EEM and the McAfee ePO Server.

- It is important to understand the export options; **Machines** and **Users** in the export wizard. You can select any one of the options to export the required user assignments from 5.x.x Endpoint Encryption Manager.
  - On selecting the **Machines** option in the export wizard, all users assigned to the selected machines from 5.x.x database are exported. This also provides the option to select specific machine, so that all the user assigned to that particular system can be exported.
  - On selecting the **Users** option in the export wizard, all systems to which the selected users are assigned are exported. This also provides the option to select specific users so that all the systems that have the selected users are exported.
- By default, system or user audit event data is not exported. It is the responsibility of the administrator to select the **Export Machine and User audit events** option during the export process.



Importing the audit logs increases the size of the McAfee ePO database. We recommend that you keep the number of days as minimum as possible.

## Import user assignments to McAfee ePO

The Endpoint Encryption Admin extension provides a user interface to import the export file (.ZIP) created during the export from 5.x.x administrator system.

### Important prerequisites for importing user assignments

- Make sure that you have the permission to **Allow Import of v5 users** to perform this task. You can enable this permission by navigating through **Menu | Users | Permission sets | Endpoint Encryption | Allow Import of v5 users**.
- Make sure that you have copied the export file (.ZIP) to a location where you can access it from the McAfee ePO server.
- Make sure that the systems to be upgraded are managed by ePolicy Orchestrator.
- Make sure to register the LDAP server on the McAfee ePO server and make sure it is the same server registered on the 5.x.x database.
- Schedule and run the server task **EE LDAP Server User/Group Synchronization** before initiating the import process.

### Key notes on importing user assignments

- If users were manually added to the 5.x.x database and the same users were not present in the Active Directory, then that 5.x.x users will appear as unmatched users in ePolicy Orchestrator during the import process. In this situation, you need to make sure that you assign these unmatched users to configured LDAP users.
- EEPC 5.x.x users disabled in the Active Directory will be imported to ePolicy Orchestrator during the import process, however, the properties of these disabled users will be determined by the Endpoint Encryption Server Setting configured in ePolicy Orchestrator.
- The application performs the system matching using the 5.x.x machine name and the McAfee ePO system name. The results are color-coordinated, so that it is easy for the administrator to analyze the results.
  - Green indicates a successful matching
  - Red indicates an unsuccessful matching
- The application performs the user matching using the binding attributes if they are present. If no match is found, the rules are used to search every LDAP server that has been set up with EE LDAP

attributes. The results are color-coordinated, so that it is easy for the administrator to analyze the results.

- Green indicates a single match
- Orange indicates more than one match
- Red indicates no match

### Do 5.x.x policies get imported to 6.2 during the migration?

No, 5.x.x policies are not imported to 6.2 as part of the migration process. The user should set the required 5.x.x policies, more importantly the **Encrypt** policy, in 6.2 before upgrading the client.



If you do not change the default **Encrypt** policy from **None** to **Encrypt** in 6.2 before the upgrade, the client system will start decrypting after the upgrade. So, it is always a best practice to configure your required policies before even initiating the import process.

### What happens if the LDAP server used by 5.x.x is not registered in ePolicy Orchestrator?

All imported users of 5.x.x will appear as unmatched users in ePolicy Orchestrator. So, ensure to register the same LDAP server used by 5.x.x, then schedule and run the **EE LDAP Server User/Group Synchronization** task.

### What happens if the LDAP server has been registered, but the EE LDAP Server User/Group Synchronization task hasn't been scheduled and run?

ePolicy Orchestrator will display an error message when the user initiates the import process. Closing the error message will guide the user directly to **EE LDAP Server User/Group Synchronization** task page.

### What happens if the 5.x.x machines are not managed by ePolicy Orchestrator?

All imported machines of 5.x.x will appear as unmatched machines in ePolicy Orchestrator. So, make sure that the systems to be migrated are managed by ePolicy Orchestrator before initiating the import process.

---

## Upgrade to EEPC 6.2

The primary goal of upgrading the EEPC 5.x.x series to EEPC 6.2 is to retain the disk encryption. This is to make sure that a decrypt and a re-encrypt of the disk is not required during the upgrade.

Only one encryption algorithm can be active for all disks, so no matter whatever the algorithm is set in 6.2, if the 5.x.x system has a different algorithm, then that algorithm will be used for all disks even after migrating to 6.2.



The only way to change the client algorithm is to deactivate EEPC on the client and decrypt all disks, then reactivate EEPC on it.

All the recovery settings have 4 times as many lines as the AES algorithm. So, setting recovery key size as **Low** gives 4 lines of response code with RC5 algorithm.

On migrating from EEPC 5.x.x to EEPC 6.2, the available user password token, SSO, and Self Recovery details are transferred to EEPC 6.2. To use 5.x.x SSO and Self Recovery data in 6.2, you need to enable Self-Recovery and SSO in the 6.2 policies after importing the users.

**What happens to a partially encrypted 5.x.x system after the migration?**

A partially encrypted 5.x.x system gets fully encrypted or decrypted as per the policies set in 6.2.

**What happens if the user initiates the upgrade process while the 5.x.x client is still in encrypting or decrypting state?**

It completes the encryption or decryption process as per the policies set in 6.2.

**What happens to a removable media that is encrypted with 5.x.x?**

We recommend that you decrypt your removable media before initiating the upgrade.



Be aware that there is no way to decrypt your removable media after the upgrade, other than using the EETech recovery tool.

**Are the 5.x.x token details migrated to 6.2?**

Yes, 5.x.x Password token details are migrated if it is available.

**Are the SSO and Self Recovery details migrated from 5.x.x to 6.2?**

Yes, the SSO and Self Recovery details are migrated from 5.x.x to 6.2 only when the 5.x.x Password token is available. The user needs to enable SSO in the 6.2 Product Settings Policy and Self-recovery in corresponding User Based Policy. The user does not have to enroll again for Self Recovery when the product is upgraded from 5.x.x to 6.2.

**What happens to a 5.x.x system after migration if it has been encrypted using an algorithm that is different from 6.2?**

The system remains encrypted with same algorithm as set in 5.x.x, and you can apply all the policies of 6.2 to the migrated system as usual.

# 7

## Use ePolicy Orchestrator to report client status

McAfee ePolicy Orchestrator provides comprehensive management and reporting tools for EEPC. Administrators can create standard and customized dashboards, queries, and reports. The procedures on how to create standard dashboards, queries, and reports are documented in the *McAfee Endpoint Encryption - 6.2 (EEPC) and 1.1 (EEMac) Product Guide*.

When the EEAgent software package is deployed to the client systems and they are successfully managed by ePolicy Orchestrator, then any of the following queries can be used to retrieve data:

- EE: Disk Status
- EE: Encryption Provider
- EE: Installed Version
- EE: Users
- EE: Product Client Events
- EE: Disk status (Rollup)
- EE: Installed version (Rollup)
- EE: Migration log
- EE: Migration lookup
- EE: Volume status
- EE: Volume status (Rollup)
- EE: V5 audit

### Contents

- [Track the progress of the deployment and encryption status](#)
- [Report encryption status from McAfee ePO](#)

---

## Track the progress of the deployment and encryption status

The progress of the EEPC deployment and the number of encrypted drives can be easily determined by running the Endpoint Encryption query under **Menu | Reporting | Queries | Endpoint Encryption | EE: Volume Status**. This will report the crypt state for all disks on systems that have the EEAgent installed.

You can also find the systems that don't have the EEAgent installed by running the query **Menu | Reporting | Queries | Endpoint Encryption | EE: Encryption Provider**.

---

## Report encryption status from McAfee ePO

To comply with data protection regulations, IT staff must be able to produce evidence that a suitable technical measure was in place to protect sensitive information on, for example, a missing computer. The organization must encrypt the device and be able to prove that the device is encrypted after it is reported lost or stolen.

### High level process

EEPC makes this task easy. An administrator can log on to McAfee ePO and, in just a few clicks, be able to produce a report showing that the missing computer was encrypted.

- Log on to ePolicy Orchestrator as an administrator.
- Locate the system in the System Tree.
- In ePolicy Orchestrator 4.5, view system properties and drill-down to encryption properties. In ePolicy Orchestrator 4.6, drill-down to encryption properties.
- Check the encryption status under the Disks tab.

**Finding the user's system in ePolicy Orchestrator**

The encryption status is stored as a property of the system, not the user. To confirm that a missing computer is encrypted, you must find the system in ePolicy Orchestrator and view its properties. You can use the queries and reports to know the encryption status of the system.



# Index

## A

- abbreviations [7](#)
- about this guide [5](#)
- activation [27](#)
- AD [14](#), [30](#)
- add local domain users [18](#), [31](#), [34–36](#)
- add users [14](#)
- Agent wake-up call [33](#)
- algorithm [45](#)
- ASCII [9](#), [10](#), [34](#), [36](#), [39](#)
- audit events [43](#)
- authentication [11](#)
- auto boot
  - configure [24](#)

## B

- backup [28](#)
- best practices [7](#)
- BIOS [11](#)
- boot sequence [11](#)

## C

- client events [47](#)
- client status [47](#)
- client system [29](#), [35](#)
- conventions and icons used in this guide [5](#)

## D

- data protection [11](#)
- default password [31](#)
- deployment [27](#), [30](#)
- deployment progress [47](#)
- design philosophy [9](#)
- disable user [35](#)
- disk check [28](#)
- disk status [47](#)
- display name [16](#)
- documentation
  - audience for this guide [5](#)
  - product-specific, finding [6](#)
  - typographical conventions and icons [5](#)

## E

- EEAdmin [29](#)
- EEAgent [10](#), [18](#), [29–31](#), [33](#)
- EEM [41](#), [43](#)
- EEPC [7](#), [11](#), [14](#), [18](#), [24](#), [27](#), [29–31](#), [33](#), [35](#), [36](#), [38](#), [39](#), [41](#), [47](#)
- EEPC extension [29](#)
- EEPC package [29](#)
- EETech [27](#), [28](#)
- Enable Automatic Booting [18](#)
- encrypted [45](#)
- encryption [7](#), [18](#), [24](#)
- encryption provider [18](#), [47](#)
- encryption status [33](#)
- Endpoint Encryption [11](#)
- export [43](#)

## G

- group users [31](#)

## H

- HDD [9](#)

## I

- import [30](#), [44](#)
- IP Address [14](#)

## L

- LDAP [14](#)
- LDAP server [13](#), [16](#), [29](#), [31](#), [35](#), [38](#), [39](#), [44](#)
- LDAP synchronization [16](#)
- Log on [18](#)

## M

- machine keys [36](#)
- machines [43](#)
- maintenance [35](#)
- MBR [11](#)
- McAfee Agent [11](#)
- McAfee ePO [11](#), [13](#), [14](#), [31](#), [33](#), [35](#), [36](#), [41](#), [43](#), [47](#)
- McAfee ServicePortal, accessing [6](#)
- migration [41](#)

**O**

Opal 9, 36  
operations 35  
OU 14, 31

**P**

password 22, 31  
PBA 7, 11, 18, 27, 31, 33–35, 41  
permission sets 38, 44  
phased deployment 13, 24  
pilot test 28  
policies  
    Product Settings Policy 10  
    User-Based Policy 10  
preparations 28  
Product Settings Policy 18, 29, 31, 34–36  
purpose 7

**Q**

queries 24, 47

**R**

readers 28  
recommendations 28  
recovery 28  
recursive 14  
report 24, 47  
reporting encryption status 47  
requirements 11  
Role Based Access Control (RBAC) 38

**S**

samaccountname 16

scalability 39  
self recovery 22, 31, 45  
server 35, 41  
server name 14  
server settings 35  
server task log 16  
ServicePortal, finding product documentation 6  
SSO 18, 33, 41  
System Tree 30

**T**

TCG 9  
Technical Support, finding product information 6  
token 28, 41, 45  
token type 10, 22

**U**

UBP enforcement  
    configure 10  
    disable 10  
    enable 10  
upgrade 41, 45  
user 28, 31, 38, 43  
user assignments 43  
user certificate 16  
User-Based Policy 22, 31  
username 16  
users 44

